PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G11B 20/00, G06F 1/00 — A1

(11) International Publication Number: WO 96/27191

(43) International Publication Date: 6 September 1996 (06.09.96)

(21) International Application Number: PCT/GB96/00447

(22) International Filing Date: 28 February 1996 (28.02.96)

(30) Priority Data:

9503996.2	28 February 1995 (28.02.95)	GB
9521765.9	24 October 1995 (24.10.95)	GB

(81) Designated States: CA, JP, US, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

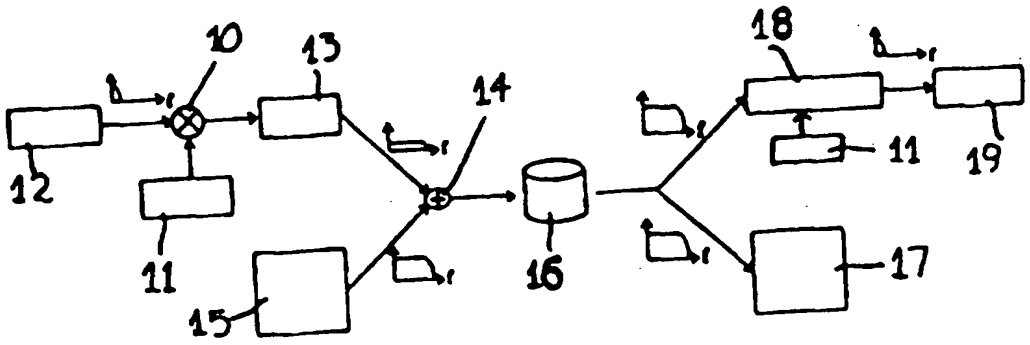
Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(71) Applicant *(for all designated States except US)*: ISIS INNOVATION LIMITED [GB/GB]; 2 South Parks Road, Oxford OX1 3UB (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: EDWARDS, David, John [GB/GB]; 9 Cooper Close, Chipping Norton, Oxfordshire OX7 5BQ (GB). STREET, Andrew, Michael [GB/GB]; 4 Clarence Road, Weymouth, Dorset DT4 9EE (GB). MOSS, Jonathan, Guy, Owen [GB/GB]; 35 Cowleigh Bank, Malvern, Worcestershire WR14 1QP (GB).

(74) Agent: PERKINS, Sarah; Stevens, Hewlett & Perkins, 1 Serjeants' Inn, Fleet Street, London EC4Y 1LL (GB).

(54) Title: COVERT IDENTIFICATION



(57) Abstract

Apparatus and a method for applying to and retrieving from a work to be protected covert identification consists of a predetermined identification (12) which is encrypted using a pseudorandom code (11). The encrypted identification is then added (14) as a noise-like feature to a signal of the work to be protected. The apparatus and method may be used to introduce covert identification into a music recording for example on a CD, literature or pictures and even into telecommunication signals. As the identification is implemented as a noise-like feature in the work, the identification cannot easily be extracted without knowledge of both the identification and the encryption code employed.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

COVERT IDENTIFICATION

The present invention relates to covert identification and in particular to a method and apparatus for applying and retrieving covert identification in a dimensional work for example an audio and/or visual media.

Increasingly security measures are being sought to protect against the unauthorised copying of copyright material and to enable the rightful holder of a copyright work to prove authorship. The business in illegal copies of popular films on video for example is believed to be significant and damaging to the film industry. In the case where authorship of an original work is in issue, it is often the case that any markings which may have been applied to the work to prove its origin may simply have been removed. Also, where only a portion of an original work has been copied or the original work has been slightly altered it is sometimes difficult to prove that copying took place.

In addition, as the move to computerised banking accelerates, the need to produce bank cards, credit cards and other printed material which cannot be successfully copied and which enable forgeries to be easily identified is now a priority for most financial organisations. This is also true of other forms of documents such as passports, security cards or travel passes.

The difficulty with most forms of security identification is that once a forger has an authorised copy to work from any security markings can be recognised and then either copied or removed. For example, in the case of banking, holograms are now applied to credit cards to deter copying of the cards. However, the technology for producing holograms is well known and easily available to someone determined to create a forgery of a credit card even if the quality of the hologram may not be the same as the original. Since the forger can see the image in the original hologram it

is that much easier for the card to be copied. However, although the hologram is present to enable the general public to identify authorised cards, in many cases the general public are not able to differentiate between an authorised copy and a forgery, even where the quality of the hologram is poor. In this case the strength of the security is dependent upon the availability of the technology involved.

Even where the security features are not visible to the naked eye, i.e. covert, inevitably information on the nature of the security markings become known and can then be copied. An example of this is the use of fluorescent markings on printed currency. The knowledge that such markings are used is now widespread which means that forgers are aware that the paper used to produce a good forgery of a bank note should also have such fluorescent markings. Similarly certain building societies in the UK include a signature of the account holder on documents which enable access to the account. The signature is transparent to visible light but may be clearly seen in ultraviolet light. This may act as a deterrent to an opportunistic pickpocket but suitable apparatus for enabling a thief to examine the covert signature is easily available and so cannot prevent money being illegally removed from an account by someone with the appropriate apparatus and an ability to copy signatures.

The present invention seeks to address the difficulties identified above with respect to conventional security measures and seeks to provide a method and apparatus for applying and retrieving covert identification in a dimensional work or record which is almost impossible to detect or reproduce without authorisation. In addition, the present invention seeks to provide a method and apparatus for applying covert identification to recorded media which are detectable even if only a portion of the recorded media is copied.

The present invention provides apparatus a method of introducing covert identification into a record comprising the steps of encrypting a

selected identification, altering a first property of the record with respect to a dimension or second property of the record in dependence on the encrypted identification and thereby generating a protected record containing noise-like perturbations of the first property.

In the context of this document reference to a record is to any work having a property susceptible to variation without loss of information. For example the record may be an audible work, such as speech or music, with the variable first property being the amplitude of the frequencies of the work. In this case the second property of the record is in the spectral dimension. Alternatively, the record may be a visual work, such as a picture, with the variable first property being the shade or intensity of the images forming the work and here the second property of the record is in the spatial dimension.

In a further alternative the record may be a compact disc (CD) with the variable first property being the reflectance of 'pits' on the surface of the CD and with the second property being in the spatial dimension.

In one preferred embodiment, the record source supplies the record in the form of an electromagnetic signal. The electromagnetic signal may be analogue or digital and the filter device may be a summator which combines the electromagnetic signal with an encrypted signal. Alternatively, the filter device may be a bank of adaptive bandpass filters which are weighted in accordance with the pseudorandom encryption of the covert identification.

Alternatively, the record may be in the form of an optical signal and the filter device may be a spatial light modulator or a phase mask.

The encryption of the covert identification is done by spread spectrum signal processing in which the identification signal is modulated by a pseudorandom sequence. This has the effect of spreading the

information in the covert identification over a known signal space or dimension. The signal space is determined by the properties of the record. Hence in the case of an audio work the signal space is in the spectral domain, whereas in the case of an optical work the signal space is in the spatial domain as it is in the case of a CD. The spreading of the information makes the resultant encrypted signal noise-like. This noise is then combined with the record and the composite appears to be the original record slightly degraded by noise. The degradation can be made to be sufficiently slight as to be negligible. The recovery of the covert identification is by means of a matched filter which reverses the noise degradation deliberately introduced. The matched filter can only be constructed with knowledge of the pseudorandom code and so the covert identification can only be extracted with knowledge of the code.

The present invention also provides apparatus for introducing covert identification into a record comprising a record source, a filter device adapted to alter a first property of the record with respect to a dimension or second property of the record in dependence on an encrypted selected identification and means for generating a protected record containing noise-like perturbations of the first property.

In a further aspect the present invention provides a method of extracting covert identification from a record comprising the steps of identifying noise-like perturbations in a first property of the record with respect to a dimension or second property of the record, extracting identified noise-like perturbations in dependence on a known encrypted selected identification and decoding the extracted noise-like perturbations to generate an output identification.

The present invention also provides apparatus for extracting covert identification from a record comprising a matched filter device having detector means for detecting noise-like perturbations in a first property of the record with respect to a dimension or second property of

the record and means for extracting detected noise-like perturbations in dependence on a known encrypted selected identification and decoding means for decoding the extracted noise-like perturbations to generate an output identification.

Embodiments of the present invention will now be described by way of example with reference to the accompanying drawings, in which:

Figure 1 is a diagram of apparatus for applying and retrieving covert identification to and from an audio recording;

Figure 2 is a diagram of apparatus for applying and retrieving covert identification to and from a digitised image;

Figure 3 shows the output of the correlator of Figure 2 without the feedback mechanism in operation;

Figure 4 shows the output of the correlator of Figure 2 with the feedback mechanism in operation for the same signal as Figure 3;

Figure 5 shows the output of the correlator of Figure 2 with the feedback mechanism in operation where the amplitude of the encrypted signal, which is the same signal as Figure 3, has been reduced;

Figure 6 shows the output of the correlator of Figure 2 with a digitised image having 63 shades of grey; and

Figure 7 shows the output of the correlator of Figure 2 with a digitised image having 220 shades of grey.

In Figure 1 apparatus is shown which enables covert identification to be combined in real-time with an audio record such as speech in a conversation or music. In the following the audio record will be referred to as the primary signal. The covert identification or fingerprint, which may be in the form of a message, is encrypted by spreading the signal in the same space dimension as the primary signal which in this case is the frequency domain. The covert identification is encrypted using a selected pseudorandom code, which is independent of the content of the covert signal, to determine the spread of the information in the covert

identification with respect to frequency. Since the encrypted signal is to be combined with the primary signal, the covert identification is encrypted with the same channel bandwidth as the primary signal.

The apparatus shown in Figure 1 may also be used to apply covert identification in real-time to a video recording. In this case the encrypted signal is applied to each frame of the video in the manner of time stamping. This also enables the covert identification to be retrieved in real-time if desired.

The apparatus includes a processor 10 connected to a source 11 of the pseudorandom code. The processor 10 also includes an input 12 which receives the covert identification or message to be encrypted. The input 12 may be in the form of a conventional alpha-numeric keyboard or a ROM. The source 11 of the pseudorandom code may be a separate processor which includes a memory in which the code, having already been generated, is stored.

The processor 10 applies the pseudorandom code to the covert message to generate an encrypted signal which is output to a filter 13. The filter 13 is a post correlation matched filter which is arranged to enhance the correlation peaks and suppress the low frequency periodic cross-correlation in the encrypted signal which could otherwise cause false alarms (i.e. a noise peak being mistaken for a correlation peak). Additional matched filters may be employed to further improve the fidelity of the covert message retrieved from the recording produced.

A device 14 for combining the encrypted signal or fingerprint signal with the primary signal is connected to the output of the filter 13 and to the source (record source) of the primary signal 15. In its simplest form the device 14 may function as a summator adding the two signals together. The amplitude or intensity of the encrypted signal is low in comparison to the primary signal, shown in Figure 1 by the relative sizes of the graphs adjacent each of the inputs to the device 14. The addition of the encrypted

signal to the primary signal results in almost negligible degradation. The combined signals are then recorded in any suitable form 16 e.g. on tape or record. As the addition of the covert identification to the primary signal does not significantly degrade the primary signal the recording may be used normally, 17. It is not necessary for the covert identification to be removed from the recording before the recording can be used.

When it is desired to authenticate the recording 16, the recording is input into a correlator 18 which may also be in the form of a processor. The correlator 18 is also connected to a source 11 of the same predetermined pseudorandom code which was used when the covert identification was originally encrypted. The correlator 18 extracts from the recording those features of the recording 16 which are features of the covert identification and not the primary signal and decodes the extracted features to recover the covert identification. The features identified may be considered as perturbations or noise in the recording 16 which can be extracted where they correlate with the encryption. The output 19 of the correlator 18 is therefore the original covert identification or message. Even where the recording 16 has been degraded, because the encrypted signal is applied to the primary signal as a very small perturbation, the encrypted signal may still be accurately extracted because the correlator 18 identifies perturbations or elements of noise in the recording rather than a specific signal. Also, as the encrypted signal is spread through the dimensional space of the primary signal, even if only a portion of the recording is available for correlation the covert identification may still be extracted.

The application of a covert identification to a primary signal may be deemed applying a 'fingerprint' to the primary signal to enable the recording to be uniquely identified. In the absence of the knowledge of the pseudorandom code used, extraction of the covert identification is virtually impossible since the features of the fingerprint signal cannot be easily

identified from the recording. Moreover absence of the covert identification in the recording would reveal the recording to be a fake.

As mentioned above the apparatus of Figure 1 may be used to apply covert identification to a video. It is also possible for images such as photographs to be similarly protected. Apparatus for introducing a covert message into a photograph is shown in Figure 2. Where appropriate common reference numerals have been used for features common to Figure 1.

With the apparatus shown in Figure 2 covert identification, for example in the form of a copyright notice, is input 12 into the processor 10. Again a source 11 of a pseudorandom code is connected to the processor 10 so that the copyright notice may be encrypted. In this case since the record or work is a two dimensional image, the copyright notice is encrypted so as to be spread through the two spatial dimensions of the image. The output of the processor 10 is applied to a filter 13 which in this case is capable of adaptively altering the power of the encrypted signal. The output of the filter 13 is then input into a summator 14 for combining the encrypted signal or fingerprint signal with a primary signal from a record source 15. The primary signal is the original image digitised. The output of the summator 14 is recorded 16, for example printed, so as to be stored in any conventional manner.

The output from the summator 14 is also used in a feedback mechanism or power control mechanism 20 which includes a correlator and secondary filter 21 which is matched to the filter 13. The correlator and secondary filter 21 are used to establish a minimum for the intensity or power of the encrypted signal without loss of information. Thus, the correlator is also connected to the source 11 of the pseudorandom code and the input 12 and the feedback mechanism 20 operates to extract the covert message from the output of the summator 14. In simple terms if the covert message is accurately extracted the power of the encrypted signal is

reduced by the adaptive filter 13, with this process being repeated until the power of the encrypted signal reaches a minimum in terms of accurate extraction of the covert message.

The apparatus for extracting the covert message from the recording 16 is similar to that of Figure 1 and consists of a correlator 18 which is connected to a source 11 of the pseudorandom code. As before the correlator extracts those features of the recording 16 which correspond to the pseudorandom code and decodes the features to recover the covert message. The output of the correlator 18 may be connected to an additional matched filter (not shown) which is used to enhance the correlation peaks identified by the correlator.

The effects of the feedback mechanism 20 are shown in Figures 3 to 5. In Figure 3 the output from the correlator 18 is shown for the first five characters of a covert message. In Figure 4 the output from the correlator 18 for the same five characters is shown where the feedback mechanism 20 is operable and with the encrypted signal having an overlaid amplitude of 4. Finally, in Figure 5 the same five characters of the covert message are shown after the feedback mechanism 20 has caused the amplitude of the encrypted signal to be reduced by the adaptive filter 13 to an overlaid amplitude of 2.

Further examples of the output from the correlator 18 for the first five characters of a covert message are shown in Figures 6 and 7 showing how the minimum required amplitude of the encrypted signal is dependent on the relative amplitude of the primary signal. In Figure 6 the primary signal is of an image having 63 shades of grey. In preliminary experiments it has been observed that the required amplitude of the encrypted signal is related to the grey scale resolution of the digitised image. With only 63 shades it was found that the fingerprint signal could be recovered with a relative amplitude as low as 1. Figure 7 shows the correlator output, after further matched filtering, for the case where the

digitised image has 220 shades of grey and in this case the encrypted signal required a relative amplitude of approximately 8 for adequate fingerprint recovery. In each case the feedback mechanism 20 has enabled the amplitude of the encrypted signal to be reduced to a minimum value without loss of information.

The above embodiments describe the application of a covert message to a digitised primary signal. In the alternative, covert identification may be applied to an audio work by passing the audio work through analogue bandpass filters which are individually and variably weighted according to the encrypted signal. In the case of an optical work, especially a photograph, the negative of the work may be exposed through a phased filter or mask the characteristics of which are determined by the encrypted covert identification. In this way the positive print produced includes the encryption.

In a further embodiment covert identification in the form of a noise-like analogue overlay is added to the digital data held on a compact disc (CD), irrespective of whether the digital data is an audio work or computer software, for example. In this case the noise-like analogue overlay is used to authenticate the CD rather than the recorded data and functions so that an unauthorised recording taken from the protected CD will not include the analogue overlay and so is recognisable as an unauthorised copy.

In a conventional CD recording, the digital data is stored in reflective 'pits' or less reflective 'islands'. When the data is initially being written onto the CD, a high powered laser is used to burn the pits in a non-reflective substrate, the remaining substrate regions becoming the islands between the pits. When the data is being read from the CD a laser reader is used to scan across the surface of the CD and a photodetector picks up the variation in reflectance from the surface of the CD. Some noise is unavoidable in this process due to the nature of the photodetector and the

amplification process. However, as the only required output is a binary signal the exact amplitude of the output signal is non-critical and so the signal is hard-limited to reproduce the original stored data. Any low-amplitude overlay would be removed by the hard-limiting process as it will appear as noise.

With this further embodiment, the length and/or width and/or location and/or depth of the individual pits in the surface of the CD are selectively altered by a small amount which in turn introduces a noise-like analogue variation in the amplitude of the reflectance from the pits when the CD is read. These alterations to the pits are made small enough that they are within the margin of error allowed in industry for the pits and may be easily introduced by modulating the power supplied to the laser writer. As with the earlier described embodiments, this modulation of the power and the resultant alteration to the pits enables a covert message or fingerprint to be introduced onto the CD. By modifying every pit by a small amount the resultant summation can produce an output large enough to be recognised by using a modified CD reader which would check for the presence or absence of the analogue overlay which involves omitting the hard-limiting performed by conventional CD players. As CDs currently hold in the order of 650MBytes of digital data, as well as some overheads such as index information, for the overlay to be easily detectable by a user with knowledge of the code, for example each bit would only need to be modified by an amount of the order of $2 \times 10^{-6}\%$.

In so far as the encryption of the covert identification is concerned, the covert identification or message may for example consist of a sequence of alphanumerics. A simple message may be built up using around 20 characters from a set of around 40 characters. The 20 characters are then encrypted and a simple technique is to use a 2047-chip M-sequence. The time diversity principle of this technique allows the character to be encoded as a time-shifted sequence. The sequence is

then overlaid with variable amplitude. The amplitude may be determined using Z=X+Y*n, where n sets the general amplitude of the encrypted signal. It will be understood though that a vast number of suitable codes and code sets are in existence and the selection of any one code may be application specific.

With the method and apparatus described it is possible for the encrypted signal to have only a small amplitude or intensity and hence a low signal to noise ratio. Since the encrypted signal has low intensity (power density) the combination of the encrypted signal with the primary signal results in noise-like perturbations with almost negligible degradation of the primary signal. Hence, without knowledge of the pseudorandom code used it is impossible to identify the covert message in the recording. However, with knowledge of the code used the covert message can be retrieved by means of correlation. The recovery of the covert message involves a processing gain which enables the encrypted signal to have the low signal to noise ratio mentioned above.

By spreading the covert identification through the primary signal space the encrypted signal includes a degree of immunity to narrowband interference and so even where the recording is subject to degradation the covert identification can still be retrieved. This is particularly important where the recording is subjected to corruption for example by compression routines on a digitised recording.

It will be readily apparent that the application of covert identification in the manner described may be utilised in a wide variety of situations. For example covert identification may be used in press agency photograph copyright policing, credit card certification, passport photograph marking, authentication of signals in telecommunications and audio and video cassette and disc protection. Also covert marking may be used to encode additional messages over primary recorded information such as audio tracks.

CLAIMS

1. A method of introducing covert identification into a record comprising the steps of encrypting a selected identification, altering a first property of the record with respect to a dimension or second property of the record in dependence on the encrypted identification and thereby generating a protected record containing noise-like perturbations of the first property.

2. A method as claimed in claim 1, further comprising the step of recording the protected record.

3. A method as claimed in either of claims 1 or 2, wherein the selected identification is encrypted using a pseudorandom code.

4. A method as claimed in claim 3, wherein the selected identification is encrypted using spread spectrum signal processing.

5. A method as claimed in any one of the preceding claims, wherein the encrypted identification is filtered to provide a filtered encryption and the first property of the record is altered in dependence on the filtered encryption.

6. A method as claimed in any one of the preceding claims, further comprising the steps of detecting the noise-like perturbations in the protected record, determining an output identification from the noise-like perturbations, comparing the output identification with the selected identification and adjusting the alteration of the first property of the record in dependence on the similarity between the output identification and the selected identification, thereby minimising the noise-like perturbations in the protected record.

7. A method as claimed in any one of the preceding claims, wherein the first property of the record is altered by filtering.

8. A method as claimed in claim 7, wherein the first property is

filtered by addition of the encrypted identification.

9. A method as claimed in claim 7, wherein the first property is filtered using a plurality of adaptive bandpass filters each of which is individually weighted in dependence on the encrypted identification.

10. A method as claimed in claim 7, wherein the first property is filtered using a spatial light modulator or phase mask.

11. A method as claimed in any one of the preceding claims, wherein the protected record is generated in real-time.

12. A method as claimed in any one of the preceding claims, wherein the first property of the record is amplitude or intensity.

13. A method as claimed in any one of the preceding claims, wherein the first property is altered with respect to the spatial or spectral dimension of the record.

14. Apparatus for introducing covert identification into a record comprising a record source, a filter device adapted to alter a first property of the record with respect to a dimension or second property of the record in dependence on an encrypted selected identification and means for generating a protected record containing noise-like perturbations of the first property.

15. Apparatus as claimed in claim 14, wherein said filter device is a summator for addition of the encrypted identification to the record.

16. Apparatus as claimed in claim 14, wherein said filter device is a plurality of adaptive bandpass filters each individually weighted in dependence on the encrypted identification.

17. Apparatus as claimed in claim 14, wherein said filter device is a spatial light modulator or phase mask.

18. Apparatus as claimed in any one of claims 14 to 17, further comprising a feedback device having detection means for detecting the noise-like perturbations in the protected record, a matched filtering device for extracting an output identification from the protected record, comparator

means for comparing the output identification with the selected identification and adaptive means for adjusting the filtering device thereby minimising the noise-like perturbations in the protected record.

19. A method of extracting covert identification from a record comprising the steps of identifying noise-like perturbations in a first property of the record with respect to a dimension or second property of the record, extracting identified noise-like perturbations in dependence on a known encrypted selected identification and decoding the extracted noise-like perturbations to generate an output identification.

20. A method as claimed in claim 19, further comprising the step of filtering the extracted noise-like perturbations.

21. Apparatus for extracting covert identification from a record comprising a matched filter device having detector means for detecting noise-like perturbations in a first property of the record with respect to a dimension or second property of the record and means for extracting detected noise-like perturbations in dependence on a known encrypted selected identification and decoding means for decoding the extracted noise-like perturbations to generate an output identification.

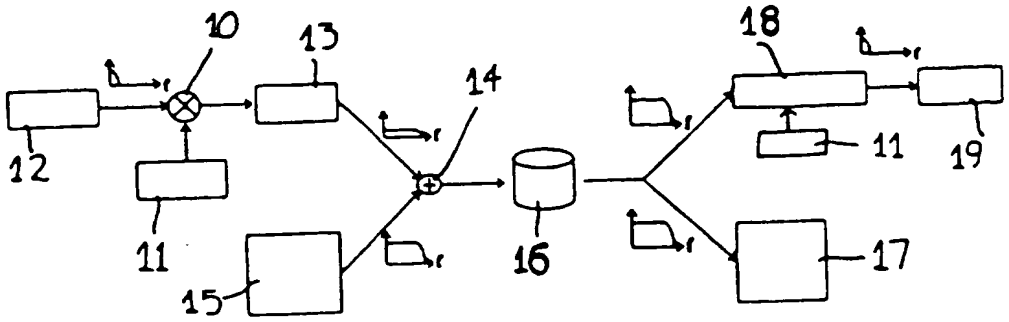


FIGURE 1

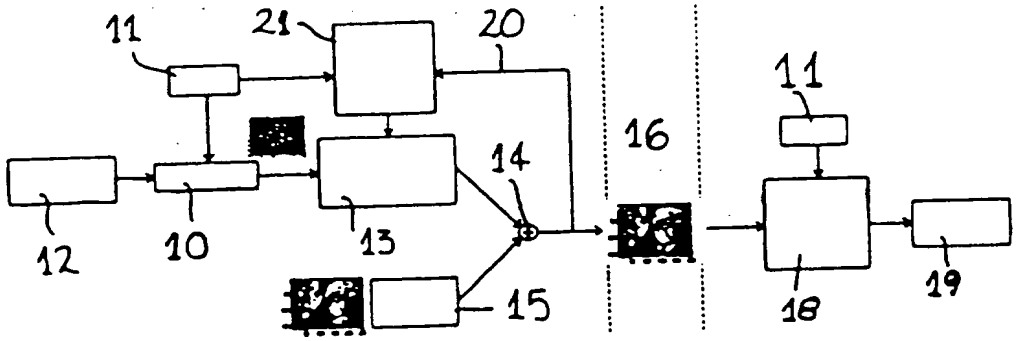


FIGURE 2

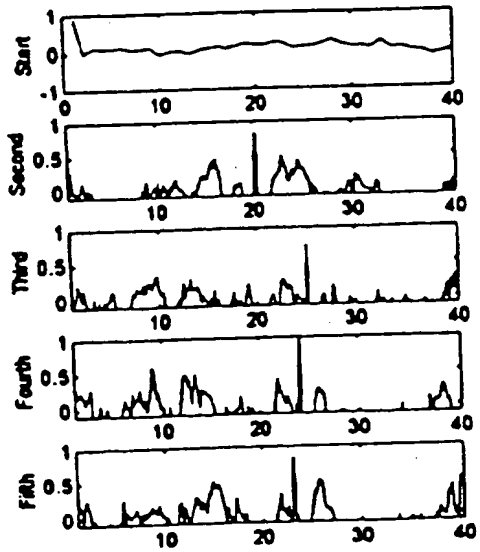


FIGURE 3

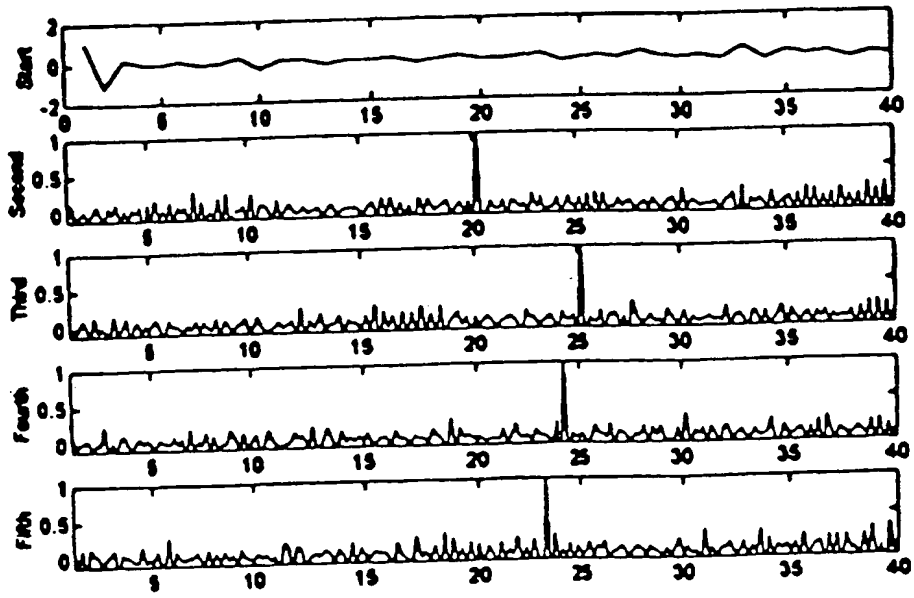


FIGURE 4

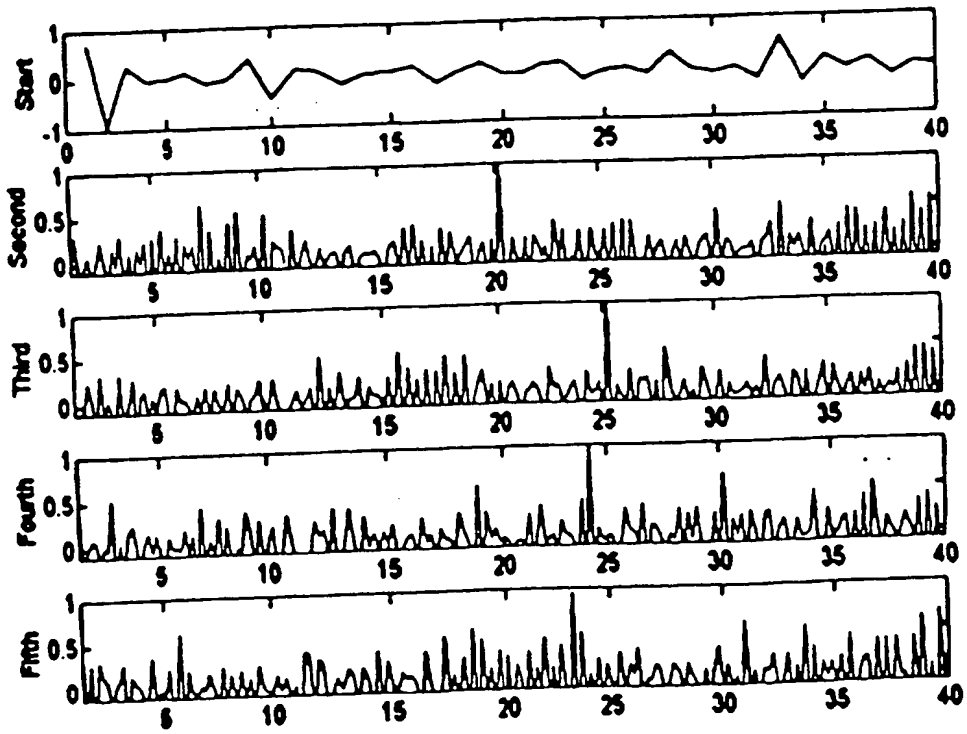


FIGURE 5

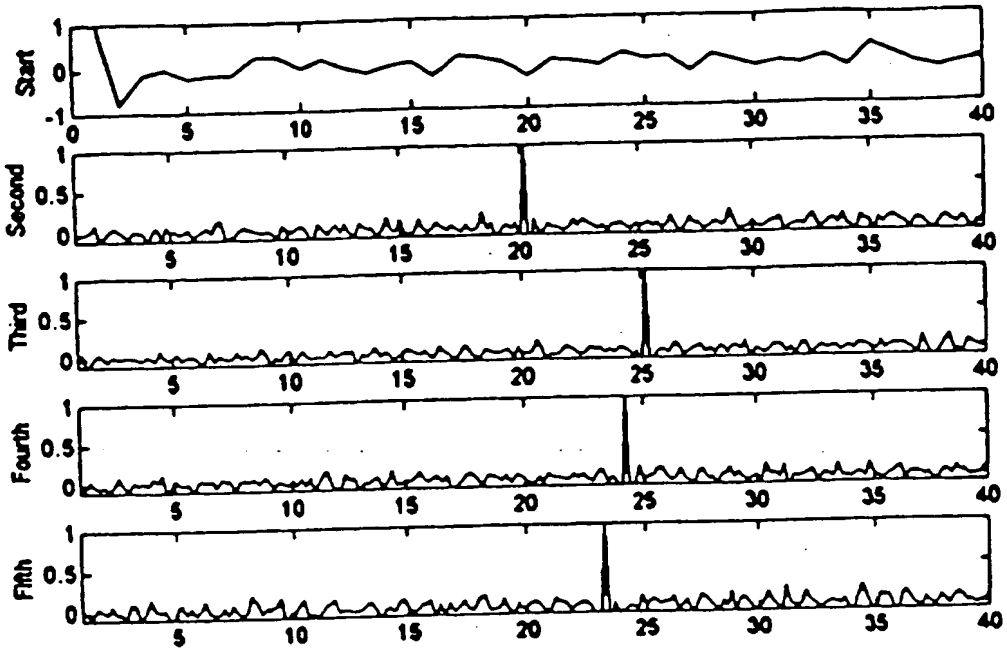


FIGURE 6

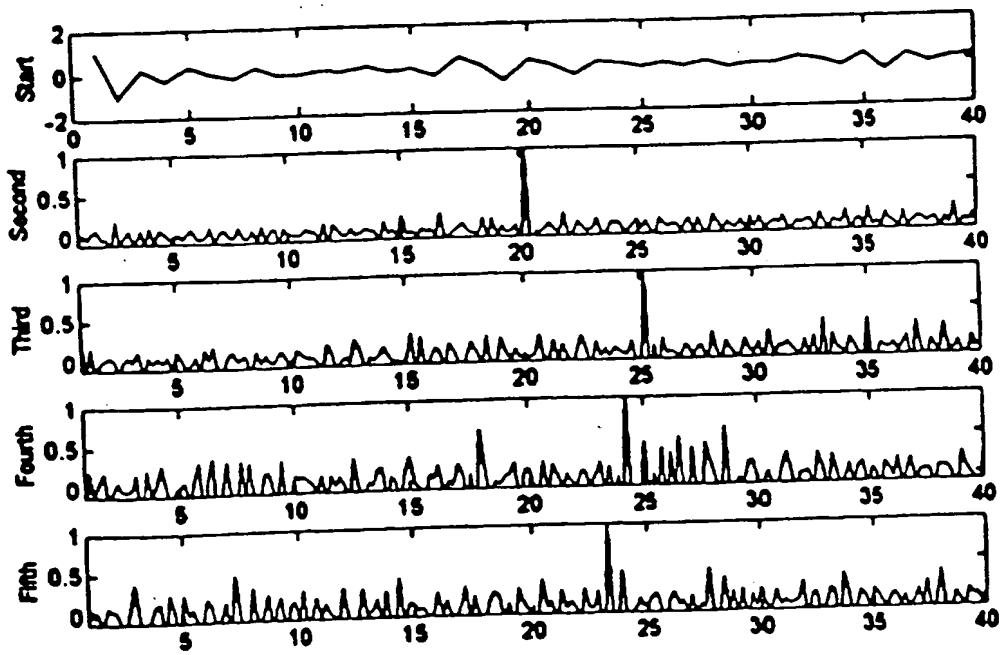


FIGURE 7

INTERNATIONAL SEARCH REPORT

Inter .nal Application No
PCT/GB 96/00447

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G11B20/00 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G11B G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO,A,93 12599 (BOLT BERANEK & NEWMAN) 24 June 1993 see the whole document ---	1-12, 14-16, 18-21
X	GB,A,2 196 167 (EMI PLC THORN) 20 April 1988 see the whole document ---	1-3,5, 11,12, 19,20
X	EP,A,0 545 472 (PHILIPS NV) 9 June 1993 see abstract see column 3, line 11 - line 45 see column 8, line 27 - column 9, line 18; figure 1 --- -/--	1,2,11, 13

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
7 June 1996	04. 07. 96

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Annibal, P

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 96/00447

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP,A,0 635 828 (VICTOR COMPANY OF JAPAN) 25 January 1995 see abstract; figure 5 ---	1,2,11, 13
A	EP,A,0 298 691 (MATSUSHITA ELECTRIC IND CO LTD) 11 January 1989 see page 3, line 20 - page 4, line 57; figures 1-3,12,13 ---	1-5,11, 12
A	US,A,4 802 212 (FREEMAN SAMUEL R ET AL) 31 January 1989 see the whole document ---	1,2,11, 12
A	FERNSEH- UND KINO-TECKNIK, vol. 42, no. 7, 1988, HEIDELBERG, DE, pages 320-322, XP002005066 BOLEWSKI: "Codierverfahren gegen Audio-Video-Piraterie" see paragraph 1.1; figure 1 ---	1,2,11, 13
A	WO,A,89 08915 (IMPERIAL COLLEGE) 21 September 1989 see page 1, paragraph 1 - page 2, paragraph 6 ---	1-3
P,X	WO,A,95 14289 (PINECONE IMAGING CORP ;RHOADS GEOFFREY B (US)) 26 May 1995 see the whole document -----	1-3,5,6, 11-13,19

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/GB 96/00447

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO-A-9312599	24-06-93	US-A-	5319735	07-06-94
		AU-B-	3320793	19-07-93
		EP-A-	0617865	05-10-94
		JP-T-	7505984	29-06-95
GB-A-2196167	20-04-88	NONE		
EP-A-0545472	09-06-93	NONE		
EP-A-0635828	25-01-95	JP-A-	7037255	07-02-95
EP-A-0298691	11-01-89	JP-A-	1014769	18-01-89
		JP-A-	1014770	18-01-89
		JP-A-	1078469	23-03-89
		JP-A-	1158668	21-06-89
		DE-D-	3851724	10-11-94
		DE-T-	3851724	04-05-95
		US-A-	4979210	18-12-90
		US-A-	5073925	17-12-91
US-A-4802212	31-01-89	NONE		
WO-A-8908915	21-09-89	AU-B-	3344289	05-10-89
		EP-A-	0406291	09-01-91
		JP-T-	3504306	19-09-91
WO-A-9514289	26-05-95	NONE		